UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/669,269	09/25/2003	Yukiyasu Tsunoo	K2291.0109	3240

32172 7590 07/09/2007

DICKSTEIN SHAPIRO LLP
1177 AVENUE OF THE AMERICAS (6TH AVENUE)
NEW YORK, NY 10036-2714

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
07/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/669,269	TSUNOO, YUKIYASU	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,22-27 and 34* is/are pending in the application.

4a) Of the above claim(s) *8-21,28-33,35 and 36* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7, 22-27 and 34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication dated 5/16/2007 with the election of claims 1-7, 22-27 and 34 and the cancellation of claims 8-21, 28-33 and 35-36.

2. Claims 1-7, 22-27 and 34 are pending.

Information Disclosure Statement

3. The information disclosure statement filed 12/20/03, 1/6/05 and 10/17/05 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Objections

4. Claims 1, 6, 22, 26 and 34 are objected to because of the following informalities:

a) As to claim 1, the phrase "a memory for storing an encryption program including the transformation tables each of which contains a predetermined number of entries" should be "a memory for storing an encryption program including the transformation tables, each of which contains a predetermined number of entries".

b) As to claim 6, the phrase "a management table containing a plurality of management entries each corresponding to the entries of the targeted transformation table" should be "a management table containing a plurality of management entries, each corresponding to the entries of the targeted transformation table".

c) As to claim 22, the phrase "comprises the steps of" should be "comprises steps of".

d) As to claim 26, the phrase "comprises the steps of" should be "comprises steps of"; "preparing a management table containing a plurality of management entries each corresponding to the entries of the targeted transformation table" should be "preparing a management table containing a plurality of management entries, each corresponding to the entries of the targeted transformation table".

e) As to claim 34, the phrase "comprises the steps of" should be "comprises steps of"; the phrase "cache memory of the computer" should be "cache memory of a computer".

Appropriate correction is required.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 22-27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 22-27 are directed to "a data encryption program instructing a cache-equipped computer to perform encryption/decryption ..." and "performing data transformation of bit strings of the given plain/cipher text". This claimed subject matter lacks a practical application of a judicial exception (law of nature, abstract idea, naturally occurring article/phenomenon) since it fails to produce a useful, concrete and tangible

result. Besides, claims 22-27 lack an appropriate computer readable storage medium to define a structural and functional interrelationship between a computer program and other elements of a computer which permits the functionality of the computer program to be realized.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

8. Claims 1-2, 4, 7, 22, 24, 27 and 34 are rejected under 35 U.S.C. 102(a) as being anticipated by Page (Theoretical Use of Cache Memory as a Cryptanalytic Side-Channel).

a) As to claim 34, Page discloses a data encryption method for performing encryption/decryption of a given plain/ciphertext using transformation tables which transforms bit strings of the given plain/cipher text (i.e. DES encryption algorithm whose core is described as pseudo-code in Fig. 2. S represents the whole S-box or substitution transformation, Page: section 4, 4.1 and 4.2), the method comprising steps of: generating the transformation tables (i.e. S-boxes), each of which contains a predetermined number of entries, wherein a targeted transformation table is previously identified from the transformation tables depending on whether the targeted transformation table exhibits a trend of increasing in the number of operation entries as

a length of encryption time becomes longer (i.e. CPU cache misses indicate the requested/targeted data must be loaded from main memory into the cache, as such a delay is generated resulting in variations in encryption time, Page: sections 2-3, pages 2-5); loading at least one part of the targeted transformation table into a cache memory of a computer (i.e. randomly loading S-box elements, Page: section 5.1); and performing data transformation of bit strings of the given plain/cipher text (Page, section 7).

b) As to claims 1 and 22, these claims are direct to a hardware/software implementation of the method of claim 34 and are rejected by a similar rationale applied against claim 34 above.

c) As to claim 2, Page discloses the entry loading section loads the at least one part of the targeted transformation table into the cache memory before the encryption/decryption of the given plain/cipher text (Page: section 5.1.).

d) As to claims 4 and 24, Page discloses the entry loading section loads all transformation tables with priorities into the cache memory, in which a transformation table with higher priority is left longer in the cache memory, wherein higher priority is assigned to the targeted transformation table compared with the other transformation tables (Page: section 2, second paragraph).

e) As to claims 7 and 27, Page discloses the targeted transformation table is identified by calculating a use rate of a number of operation entries to a total number of entries for each of the transformation tables (i.e. cache miss is the data not contained in the cache and must be fetched from main memory (Page: Section 2, page 4) and the

example attack is based on accesses to the S-box structures with the value of these S-boxes is fetched from a table in memory. This means the access to memory will be routed through the cache and produce an access profile without which such attacks are useless (Page: section 3, page 5, first paragraph) and selecting a transformation table having a smaller use rate as the targeted transformation table (i.e. the smaller the use rate the more appropriate to select and store those as the targeted transformation table because if the use rate is high, then it should be considered as cache hit, Page: section 2).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 3 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Page (Theoretical Use of Cache Memory as a Cryptanalytic Side-Channel).

Page discloses the entry loading section loads all transformation tables into the cache memory (Page: section 5.1), however he is silent on the capability of having the targeted transformation table is loaded after the other transformation tables have been loaded into the cache memory.

The examiner takes official notice that the use of having the targeted transformation table is loaded after the other transformation tables have been loaded

into the cache memory (i.e. last-in-first-out (LIFO) memory) in the system of Page so as to easily access the targeted transformation table.

11. Claims 5 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Page (Theoretical Use of Cache Memory as a Cryptanalytic Side-Channel) in view of Lee (6,654,874).

Page discloses the method of claim 2, however he is silent on the capability of having the entry loading section loads the at least one part of the targeted transformation table into the cache memory at a plurality of timings before the encryption/decryption of the given plain/cipher text. Lee is relied on for the teaching of having the entry loading section loads the at least one part of the targeted transformation table into the cache memory at a plurality of timings before the encryption/decryption of the given plain/cipher text (Lee: col. 9, lines 1-15). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the entry loading section loads the at least one part of the targeted transformation table into the cache memory at a plurality of timings before the encryption/decryption of the given plain/cipher text in the system of Page, as Lee teaches so as to increase performance loss and current consumption of the microcomputer (Lee: col. 9, lines 22-23).

12. Claims 6 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Page (Theoretical Use of Cache Memory as a Cryptanalytic Side-Channel) in view of Ng et al. (6,725,329).

Page discloses the method of claim 1, however he is silent on the capability of having a management table containing a plurality of management entries, each corresponding to the entries of the targeted transformation table, each management entry indicating whether a corresponding entry of the targeted transformation table has been used; and a unused-entry manager for loading unused entries of the targeted transformation table into the cache memory by referencing the management table. Ng is relied on for the teaching of having a management table containing a plurality of management entries, each corresponding to the entries of the targeted transformation table, each management entry indicating whether a corresponding entry of the targeted transformation table has been used; and a unused-entry manager for loading unused entries of the targeted transformation table into the cache memory by referencing the management table (Ng: col. 2, lines 59-61; Fig. 2; Fig. 5; col. 5, lines 9-67). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a management table containing a plurality of management entries, each corresponding to the entries of the targeted transformation table, each management entry indicating whether a corresponding entry of the targeted transformation table has been used; and a unused-entry manager for loading unused entries of the targeted transformation table into the cache memory by referencing the management table in the system of Page, as Ng teaches, so as to efficiently allocate

and configure memory segments for responding to host commands (Ng: col. 1, lines 39-42).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
6/20/07